Public Key Cryptography Options for Trusted Host Identities in HIP

Harri Forsgren and Timo Karvi
University of Helsinki, Department of Computer Science
Kaj Grahn and Göran Pulkkis
Arcada University of Applied Sciences

WISEciti Public Seminar 19.5.2010

Outline

- Trust and Host Identities (HIs)
- PKI Certified HIs
- HI Trust derived from DNSSEC
- IBE (Identity based Public Key Cryptography) HIs
- CL-PKC (Certificate-less Public Key Cryptography) HIs
- Conclusions

Trust and Host Identities (HIs)

From **"Security, Trust, Dependability and Privacy in Wireless and Mobile Telecommunications, White Paper, eMobility Strategic Research Agenda, 7th Framework Programme, EU December 2008":**

- Trust is a complex concept that is composed of many different attributes, such as reliability, dependability, honesty, truthfulness, security, competence and timeliness, which may have to be considered depending on the actual environment.
- It must be noted that trust is directed, highly subjective, context-dependent, dynamic and conditionally transferable, and also depends on history.
- **Trust should be obtained, perceived, assessed, measured, ensured and communicated.**

Trust and Host Identities (HIs)

- How can a HIP host be sure that a Base Exchange peer is legitimate and not malicious?
- Neither PKI certification of HIs nor any other method to derive trust in His is included in current architecture and protocol specifications of HIP
- Trust in a HI can be derived from a TTP (Trusted Third Party) since a HI is specified to be a public/private key pair. A TTP is
  - a CA (Certification Authority) for a PKI certified HI
  - DNSSEC for a HI registered in DNS
  - A PKG (Private Key Generation authority) for an IBE (Identity based Public Key Cryptography) HI and a CL-PKC (Certificate-less Public Key Cryptography) HI

PKI Certified Host Identities (HIs)

- HI certification by 'globally trusted' CAs creates a trust relationship in Base Exchange between two HIP hosts
- Also intra-domain trusted CA certification creates such a trust relationship, in Base Exchange between two HIP hosts, when domains of both HIP hosts belong to the same **ID Management Federation** (Microsoft CardSpace, OpenID, Liberty Alliance, Shibboleth)
- 'globally trusted' CA is a fuzzy concept – a CA is assumed to be 'globally trusted' if the corresponding CA certificate is included in the set of preinstalled CA certificates in the certificate database of a www browser or an e-mail client

PKI Certified Host Identities (HIs)

PKI certification of HIs is not included in architecture or protocol specifications for HIP, but a CERT parameter is defined in protocol specifications and further specified in an IETF draft

- A HIP packet may contain one or multiple CERT parameters for certificates of type X.509.v3 or SPKI
- PKI certification of HIs adds HI certificate verification and an online revocation list check to HIP signature verification

HI Trust derived from DNSSEC

- An initiator host needs before a Base Exchange a response to a DNS query in order to get a the IP, HI and HIT of a responder host
- The initiator can be trapped in Base Exchange with a malicious host if DNS is forged or the response to the DNS query is tampered
- Forging of DNS and tampering of DNS messages is prevented by DNSSEC: a DNSSEC query returns the IP, HI and HIT of the responder in a message signed by the DNSSEC server
- Trust derived from a DNSSEC signature is trust of the initiator host in the HI and HIT of the responder host. No trust of the responder host in the HI of the initiator host in a Base Exchange can be retrieved from DNSSEC signatures

IBE (Identity based Public Key Cryptography) HIs

HIP architecture specifications:

- any name that can claim to be 'statistically globally unique' may serve as a Host Identifier (HI)
- a public key of a 'public key pair' makes the best HI.

Both requirements are fulfilled using Identity based Public Key Cryptography (IBE):

- The public key chosen to be a HI is a globally unique identity string for a HIP host, for example FQDN or NAI
- Trust in an IBE based HI is derived from a trusted Private Key Generation authority (PKG), from which a HIP host gets the private key corresponding to the identity string chosen as HI

IBE (Identity based Public Key Cryptography) HIs

- Private Key Escrow: the private key of a HIP host is also known by the PKG. Such private key escrow can be avoided by using threshold techniques in distributed generation of private HI keys
- Inclusion of IBE signature algorithm (based on pairing of discrete points on elliptic curves) in HIP specifications and implementations
- Public parameters of PKG used by a HIP peer host are needed in HIP signature verification in Base Exchange between two HIP hosts using different PKGs
  - Exchange of public PKG parameters in Base Exchange messages R1 and I2
  - Trust in PKG used by a peer HIP host by PKI certification of exchanged public PKG parameters

CL-PKC (Certificate-less Public Key Cryptography) HIs

CL-PKC is a modification of IBE:

- a hash of an identity string with a public hash function is a ***partial public key*** of a HIP host
- a PKG generates a ***partial private key*** for the partial public key, which is securely delivered to the HIP host
- the HIP host chooses a secret integer, which is embedded in the private and public keys derived from the partial keys
  - no private key escrow as in IBE
  - the HI is an identity string uniquely modified by the HIP host

CL-PKC (Certificate-less Public Key Cryptography) HIs

- Inclusion of CL-PKC signature algorithm (as in IBE - based on pairing of discrete points on elliptic curves) in HIP specifications and implementations
- Public parameters of PKG used by a HIP peer host are - as in IBE - needed in HIP signature verification in Base Exchange between two HIP hosts using different PKGs
  - Exchange of public PKG parameters in Base Exchange messages R1 and I2
  - Trust in a PKG used by a peer HIP host by PKI certification of exchanged public PKG parameters

Conclusions

- Trust in a HI can be retrieved from a Trusted Third Party (TTP) by certification of
  - the public key of the HI which is a public/private key pair (PKI trust)
  - the retrieval of the public key of the HI (DNSSEC trust)
  - HI generation (PKG trust)
- PKI trust in a HI requires certificate chain verification and online revocation check for each HIP signature
- DNSSEC trust and PKG trust require only one certificate chain verification and online revocation check for each HIP session and revocation list are short (DNSSEC servers a nd PKGs)
- DNSSEC trust is only HIP initiator trust in a HIP responder
- PKG trust is mutual between a HIP initiator and a HIP responder but requires the use of IBE or CL-PKC

Thank you for your attention!

Questions?

Comments?